

ARTICLES DE LOI RGPD ET LPD CONCERNANT L'ANALYSE D'IMPACT

RGPD - Analyse d'impact relative à la protection des données et consultation préalable

Article 35 Analyse d'impact relative à la protection des données

1. Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires.

2. Lorsqu'il effectue une analyse d'impact relative à la protection des données, le responsable du traitement demande conseil au délégué à la protection des données, si un tel délégué a été désigné.

3. L'analyse d'impact relative à la protection des données visée au paragraphe 1 est, en particulier, requise dans les cas suivants:

a) l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire;

b) le traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10; ou

c) la surveillance systématique à grande échelle d'une zone accessible au public.

4. L'autorité de contrôle établit et publie une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise conformément au paragraphe 1. L'autorité de contrôle communique ces listes au comité visé à l'article 68.

5. L'autorité de contrôle peut aussi établir et publier une liste des types d'opérations de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise. L'autorité de contrôle communique cette liste au comité.

6. Avant d'adopter les listes visées aux paragraphes 4 et 5, l'autorité de contrôle compétente applique le mécanisme de contrôle de la cohérence visé à l'article 63, lorsque ces listes comprennent des activités de traitement liées à l'offre de biens ou de services à des personnes concernées ou au suivi de leur comportement dans plusieurs États membres, ou peuvent affecter sensiblement la libre circulation des données à caractère personnel au sein de l'Union. 4.5.2016 L 119/53 Journal officiel de l'Union européenne FR

7. L'analyse contient au moins: a) une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement; b) une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités; c) une évaluation des risques pour les droits et libertés des personnes concernées conformément au paragraphe 1; et d) les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

8. Le respect, par les responsables du traitement ou sous-traitants concernés, de codes de conduite approuvés visés à l'article 40 est dûment pris en compte lors de l'évaluation de l'impact des opérations de traitement effectuées par lesdits responsables du traitement ou sous-traitants, en particulier aux fins d'une analyse d'impact relative à la protection des données.

9. Le cas échéant, le responsable du traitement demande l'avis des personnes concernées ou de leurs représentants au sujet du traitement prévu, sans préjudice de la protection des intérêts généraux ou commerciaux ou de la sécurité des opérations de traitement.

10. Lorsque le traitement effectué en application de l'article 6, paragraphe 1, point c) ou e), a une base juridique dans le droit de l'Union ou dans le droit de l'État membre auquel le responsable du traitement est soumis, que ce droit règlemente l'opération de traitement spécifique ou l'ensemble des opérations de traitement en question et qu'une analyse d'impact relative à la protection des données a déjà été effectuée dans le cadre d'une analyse d'impact générale réalisée dans le cadre de l'adoption de la base juridique en question, les paragraphes 1 à 7 ne s'appliquent pas, à moins que les États membres n'estiment qu'il est nécessaire d'effectuer une telle analyse avant les activités de traitement.

11. Si nécessaire, le responsable du traitement procède à un examen afin d'évaluer si le traitement est effectué conformément à l'analyse d'impact relative à la protection des données, au moins quand il se produit une modification du risque présenté par les opérations de traitement.

Article 36 Consultation préalable

1. Le responsable du traitement consulte l'autorité de contrôle préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données effectuée au titre de l'article 35 indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque.

2. Lorsque l'autorité de contrôle est d'avis que le traitement envisagé visé au paragraphe 1, constituerait une violation du présent règlement, en particulier lorsque le responsable du traitement n'a pas suffisamment identifié ou atténué le risque, l'autorité de contrôle fournit par écrit, dans un délai maximum de huit semaines à compter de la réception de la demande de consultation, un avis écrit au responsable du traitement et, le cas échéant, au sous-traitant, et peut faire usage des pouvoirs visés à l'article 58. Ce délai peut être prolongé de six semaines, en fonction de la complexité du traitement envisagé. L'autorité de contrôle informe le responsable du traitement et, le cas échéant, le sous-traitant de la prolongation du délai ainsi que des motifs du retard, dans un délai d'un mois à compter de la réception de la demande de consultation. Ces délais peuvent être suspendus jusqu'à ce que l'autorité de contrôle ait obtenu les informations qu'elle a demandées pour les besoins de la consultation.

3. Lorsque le responsable du traitement consulte l'autorité de contrôle en application du paragraphe 1, il lui communique:

a) le cas échéant, les responsabilités respectives du responsable du traitement, des responsables conjoints et des sous-traitants participant au traitement, en particulier pour le traitement au sein d'un groupe d'entreprises; b) les finalités et les moyens du traitement envisagé; c) les mesures et les garanties prévues afin de protéger les droits et libertés des personnes concernées en vertu du présent règlement; d) le cas échéant, les coordonnées du délégué à la protection des données; e) l'analyse d'impact relative à la protection des données prévue à l'article 35; et f) toute autre information que l'autorité de contrôle demande.

4. Les États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement.

5. Nonobstant le paragraphe 1, le droit des États membres peut exiger que les responsables du traitement consultent l'autorité de contrôle et obtiennent son autorisation préalable en ce qui concerne le traitement effectué par un responsable du traitement dans le cadre d'une mission d'intérêt public exercée par celui-ci, y compris le traitement dans le cadre de la protection sociale et de la santé publique.

Loi fédérale sur la protection des données (LPD teneur automne 2020)

Art. 22 Analyse d'impact relative à la protection des données personnelles

¹ Lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, le responsable du traitement procède au préalable à une analyse d'impact relative à la protection des données personnelles. S'il envisage d'effectuer plusieurs opérations de traitement semblables, il peut établir une analyse d'impact commune.

² L'existence d'un risque élevé, en particulier lors du recours à de nouvelles technologies, dépend de la nature, de l'étendue, des circonstances et de la finalité du traitement. Un tel risque existe notamment dans les cas suivants:

- a. traitement de données sensibles à grande échelle;
- b. surveillance systématique de grandes parties du domaine public.

³ L'analyse d'impact contient une description du traitement envisagé, une évaluation des risques pour la personnalité ou les droits fondamentaux de la personne concernée, ainsi que les mesures prévues pour protéger sa personnalité et ses droits fondamentaux.

⁴ Le responsable du traitement privé est délié de son obligation d'établir une analyse d'impact s'il est tenu d'effectuer le traitement en vertu d'une obligation légale.

⁵ Le responsable du traitement privé peut renoncer à établir une analyse d'impact lorsqu'il recourt à un système, un produit ou un service certifié conformément à l'art. 13 pour l'utilisation prévue ou qu'il respecte un code de conduite au sens de l'art. 11 remplissant les conditions suivantes:

- a. il repose sur une analyse d'impact relative à la protection des données personnelles;
- b. il prévoit des mesures pour protéger la personnalité et les droits fondamentaux de la personne concernée;
- c. il a été soumis au PFPDT.

Art. 23 Consultation préalable du PFPDT

¹ Le responsable du traitement consulte le PFPDT préalablement au traitement lorsque l'analyse d'impact relative à la protection des données révèle que, malgré les mesures prévues par le responsable du traitement, le traitement envisagé présente encore un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée.

² Le PFPDT communique au responsable du traitement ses objections concernant le traitement envisagé dans un délai de deux mois. Ce délai peut être prolongé d'un mois lorsqu'il s'agit d'un traitement de données complexe. Protection des données. LF FF 2020

³ Si le PFPDT a des objections concernant le traitement envisagé, il propose au responsable du traitement des mesures appropriées.

⁴ Le responsable du traitement privé peut renoncer à consulter le PFPDT s'il a consulté son conseiller à la protection des données au sens de l'art. 10.

*